UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/749,742	12/28/2000	John W. Marshall	SSB0001-US	5548

27510   7590   05/18/2005

KILPATRICK STOCKTON LLP
607 14TH STREET, N.W.
WASHINGTON, DC 20005

EXAMINER
DINH, MINH

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 05/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	Application No.	Applicant(s)
	09/749,742	MARSHALL ET AL.
	Examiner	Art Unit	
	Minh Dinh	2132	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>31 January 2005</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-20</u> is/are pending in the application.

4a)·Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) <u>19 and 20</u> is/are allowed.

6)☒ Claim(s) <u>1-18</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>28 December 2000</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)   4)☐ Interview Summary (PTO-413)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)   Paper No(s)/Mail Date. _____.
3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)   5)☐ Notice of Informal Patent Application (PTO-152)
   Paper No(s)/Mail Date _____.   6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   This action is in response to the amendment filed 07/07/2004. Claims 19-20

have been added.

Response to Arguments

2.   Applicant's arguments filed 07/07/2004 have been fully considered but they are

not persuasive. Applicant argues that Zeichick does not disclose a globally replicated

public folder within the electronic messaging system for refreshing the local

configuration (page 9). Zeichick discloses that a package including new virus definition

and improved program files is downloaded from the Symantec server to a LiveUpdate

server and then to each client in the electronic messaging system. The package

includes multiple files and, therefore, is functionally equivalent to a folder. The package

is publicly available and is globally downloaded to all enterprise mail clients (p. 4, "A key

element of NAV ... once per day from the LiveUpdate server"; "NAV Corporate 7.01

supports ... popular enterprise mail clients").

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed
> publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4.   Claims 1 and 9 are rejected under 35 U.S.C. 102(a) as being anticipated by

Zeichick ("Content Security – Keep Your Users Safe... And Focused – Three software

packages aim to keep your employee's eyes front and center").

Regarding claim 1, Zeichick discloses a method comprising: implementing a

security software application in an electronic messaging system with connection to a

data network (p. 3, "Symantec's Norton AniVirus ... NAV works to stop it at that point");

providing a local configuration of the security software application on a local messaging

terminal, wherein the local configuration includes a list of at least one known malicious

application (p. 4, "A key element of NAV ... locally to NAV Corporate clients"); detecting

an electronic message received or to be sent by a local messaging terminal (p. 3,

"Symantec's Norton AniVirus ... NAV works to stop it at that point"); determining

whether the electronic message includes any attachment (p. 4, "Now that the servers ...

Mail 8.0 and 8.1"); if an attachment is included with the electronic message, using the

security software application to check the attachment for any malicious application

based on the list of at least one known malicious application (p. 4, "Now that the servers

... and it did so"); refreshing the local configuration of the security software application

from a globally replicated public folder within the electronic messaging system on a

desired periodic basis (p. 4, "A key element of NAV ... once per day from the

LiveUpdate server"; "NAV Corporate 7.01 supports ... popular enterprise mail clients").

Regarding claim 9, Zeichick further discloses that the local configuration of the

security software application includes an option to set a time for the desired periodic

basis to refresh the local configuration (p. 4, "A key element of NAV ... once per day

from the LiveUpdate server").

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Zeichick as applied to claim 1 above, and further in view of "The University of Texas at

Austin Chooses CA's InoculateIT to Protect Web Environment Against Virus Attacks".

Regarding claim 2, Zeichick does not disclose implementing an add-in software

component to an electronic message client of the electronic messaging system. The

"The University of Texas" reference discloses implementing an add-in software

component to an electronic message client of an electronic messaging system (p. 2,

"After evaluating several different ... the virus-free environment." and p.3, "To add yet

another layer ... enter the school's email system"). It would have been obvious to one

of ordinary skill in the art at the time the invention was made modify the Zeichick

method to implement an add-in software component to an electronic message client of

the electronic messaging system, as disclosed in the reference "The University of

Texas", to provide more robust virus detection capabilities to the mail system.

Regarding claim 3, Zeichick further discloses that the electronic message client

software resides in a host server (p. 4, "The downside with the ... Mail 8.0 and 8.1").

7.   Claims 4-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Zeichick as applied to claim 1 above, and further in view of Ji et al. (5,889,943).

Regarding claim 4, Zeichick does not disclose that the security software

application includes a dynamic link library (DLL) application. Ji discloses a security

software application includes a dynamic link library (DLL) application (col. 11, lines 38-

44). It would have been obvious to one of ordinary skill in the art at the time the

invention was made modify the Zeichick method such that the security software

application includes a dynamic link library (DLL) application, as taught by Ji, to utilize a

shared library.

Regarding claim 5, Zeichick does not disclose prompting an error message on

the local messaging terminal when the attachment to the electronic message matches a

name on the list of the at least one known malicious application. Ji discloses alerting

the recipient of an electronic message when an attachment to the electronic message

contains a virus (col. 20, lines 48-63); Ji's teaching meets the limitation of the claim. It

would have been obvious to one of ordinary skill in the art at the time the invention was

made modify the Zeichick method to prompt an error message on the local messaging

terminal when the attachment to the electronic message matches a name on the list of

the at least one known malicious application, as taught by Ji, to alert the recipient.

Regarding claim 6, Zeichick does not disclose blocking the matched attachment from being opened or sent. Ji discloses blocking the matched attachment from being opened (col. 12, lines 48-63). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the Zeichick method to block the matched attachment from being opened, as taught by Ji, so that the virus would not be activated.

8.   Claims 7-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zeichick as applied to claim 1 above, and further in view of Komiega ("Storage product prevents virus attacks").

Regarding claim 7, Zeichick does not explicitly disclose that the list of at least one known malicious application includes a list of known virus file names. Komiega discloses a list of known virus file names being utilized to block known virus files (p. 3, "Although FileScreen 2000 will ... block the file by its names"). It would have been obvious to one of ordinary skill in the art at the time the invention was made modify the Zeichick method to utilize a list of known virus file names, as taught by Komiega, in order to block known virus files.

Regarding claim 8, Zeichick discloses that the local configuration of the security software application includes an option to enable a checking of an attachment for any malicious application based on the list of at least one known malicious application (p. 4, "End users wishing to ... is needlessly complex").

Zeichick does not disclose that the local configuration includes an option to add or remove a known malicious application from the list of at least one known malicious

application and an option to restrict an attachment type. Komiega discloses an option to

add a known malicious application to the list of at least one known malicious application

files and an option to restrict an attachment type (p. 3, "Although FileScreen 2000 will ...

block the file by its names"). It would have been obvious to one of ordinary skill in the

art at the time the invention was made modify the Zeichick method such that that the

local configuration includes an option to add or remove a known malicious application

from the list of at least one known malicious application and an option to restrict an

attachment type, as taught by Komiega, in order to provide options for blocking known

virus files or certain attachment types that may contains a virus.

9.   Claims 10, 13-15 and 18 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Zeichick in view of Komiega.

        Regarding claim 10, Zeichick discloses a method comprising: implementing a

security software application in an electronic messaging system with connection to a

data network (p. 3, "Symantec's Norton AniVirus ... NAV works to stop it at that point");

providing a local configuration of the security software application on a local messaging

terminal, wherein the local configuration includes a list of at least one known malicious

application (p. 4, "A key element of NAV ... locally to NAV Corporate clients"); detecting

an electronic message received or to be sent by a local messaging terminal (p. 3,

"Symantec's Norton AniVirus ... NAV works to stop it at that point"); determining

whether the electronic message includes any attachment (p. 4, "Now that the servers ...

Mail 8.0 and 8.1"); if an attachment is included with the electronic message, using the

security software application to check the attachment for any malicious application

based on the list of at least one known malicious application (p. 4, "Now that the servers

... and it did so"); refreshing the local configuration of the security software application

from a globally replicated public folder within the electronic messaging system on a

desired periodic basis (p. 4, "A key element of NAV ... once per day from the

LiveUpdate server"; "NAV Corporate 7.01 supports ... popular enterprise mail clients").

Zeichick does not disclose that the local configuration includes at least one

application type. Komiega discloses a method for blocking e-mail attachments of one of

executable application types included in a local configuration (p. 2, "According to David

Hill ... for use by an end user." and p. 3, "W. Quinn's FileScreen 2000 ... to block the file

by its file name"). It would have been obvious to one of ordinary skill in the art at the

time the invention was made modify the Zeichick method such that the local

configuration includes at least one executable application type and the local

configuration is used to block e-mail attachments of certain types, as taught by

Komiega, so that users would not be allowed to receive e-mail attachments that have an

extension that may contain a virus.

Regarding claim 13, Zeichick discloses that the local configuration of the security

software application includes an option to enable a checking of an attachment for any

malicious application based on the list of at least one known malicious application (p. 4,

"End users wishing to ... is needlessly complex"). Zeichick does not disclose that the

local configuration includes an option to add or remove an application type from the list

of at least one application type and an option to enable a checking of an attachment for

a restricted application type based on the list of at least one application type. It would

have been obvious to one of ordinary skill in the art at the time the invention was made

modify the Zeichick method such that the local configuration includes an option to add

or remove an application type from the list of at least one application type and an option

to enable a checking of an attachment for a restricted application type based on the list

of at least one application type, as taught by Komiega. Please refer to motivation

recited for including at least one executable application type in the local configuration as

taught by Komiega in claim 10.

Claims 14-15 are rejected on the same basis as claim 10.

Regarding claim 18, Zeichick further discloses that the local configuration of the

security software application includes an option to set a time for the desired periodic

basis to refresh the local configuration (p. 4, "A key element of NAV ... once per day

from the LiveUpdate server").

10.   Claims 11-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Zeichick in view of Komiega as applied to claim 10 above, and further in view of "The

University of Texas at Austin Chooses CA's InoculateIT to Protect Web Environment

Against Virus Attacks".

Regarding claim 11, Zeichick does not disclose implementing an add-in software

component to an electronic message client of the electronic messaging system. The

"The University of Texas" reference discloses implementing an add-in software

component to an electronic message client of an electronic messaging system (p. 2,

"After evaluating several different ... the virus-free environment" and p.3, "To add yet

another layer ... enter the school's email system"). It would have been obvious to one

of ordinary skill in the art at the time the invention was made modify the Zeichick

method to implement an add-in software component to an electronic message client of

the electronic messaging system, as disclosed in the reference "The University of

Texas", to provide more robust virus detection capabilities to the mail system.

Regarding claim 12, Zeichick further discloses that the electronic message client

software resides in a host server (p. 4, "The downside with the ... Mail 8.0 and 8.1").

11.   Claims 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Zeichick in view of Komiega as applied to claim 10 above, and further in view of Ji.

Zeichick and Komiega do not disclose that the list of at least one application type

comprises application types not capable of containing malicious applications and that if

the attachment is of one of the application types not capable of containing malicious

applications, allowing the attachment to be opened or sent through the electronic

messaging system. Ji discloses that the list of at least one application type comprises

application types not capable of containing malicious applications and that if the

attachment is of one of the application types not capable of containing malicious

applications, allowing the attachment to be opened or sent through the electronic

messaging system (col. 19, lines 45-51). It would have been obvious to one of ordinary

skill in the art at the time the invention was made modify the combined method of

Zeichick and Komiega such that that the list of at least one application type comprises

application types not capable of containing malicious applications and that if the

attachment is of one of the application types not capable of containing malicious

applications, allowing the attachment to be opened or sent through the electronic

messaging system, as taught by Ji, to make the scanning process more efficient.

Allowable Subject Matter

12.   Claims 19-20 are allowed.

13.   The following is a statement of reasons for the indication of allowable subject

matter. Claims 19-20 are directed to a method of updating virus definition used by anti-

virus software for scanning electronic mails. Independent claim 19 identifies the

uniquely distinct features: "detecting a receipt of an electronic message sent to the local

messaging terminal; determining whether the electronic message includes any

attachment; upon the determining that an attachment is included with the electronic

message, determining whether a time period since a last update of the local

configuration has passed beyond a predetermined threshold period; and upon the

determining that the time period since the last update of the local configuration has

passed beyond the predetermined threshold period, updating the local configuration

from a globally replicated public folder within the electronic messaging system". The

closest prior art, Zeichick ("Content Security – Keep Your Users Safe... And Focused –

Three software packages aim to keep your employee's eyes front and center"),

discloses that anti-virus software at the clients are configured to download the new virus

definition on a desired periodic basic such as once per day. Another prior art, Hodges

et al (6,269,456), discloses that the updating process is performed whenever a client is

connected to the Internet. The prior art, taken either singly or in combination, fails to

anticipate or fairly suggest the limitations of applicant's independent claim, in such a

manner that a rejection under 35 U.S.C 102 or 103 would be proper. The claimed

invention is therefore considered to be in condition for allowance as being novel and

nonobvious over prior art.

Conclusion

14.   The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

U.S. Patent No. 6,269,456 to Hodges et al.

U.S. Patent No. 6,728,886 to Ji et al.

U.S. Patent No. 6,757,830 to Tarbotton et al.

Drips, "Pair of Products Protects E-mail And Attachments"

15.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.
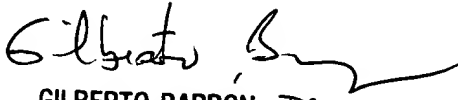
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD

Minh Dinh
Examiner
Art Unit 2132

MD
5/13/05

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100